AKO TO VIDÍME MY...

Dott. Andrej Aleksiev, PhD.

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT
INFINITY

C L O U D • M O B I L E • T H R E A T P R E V E N T I O N

Last update Q3/19

CYBER
SECURITY
TODAY

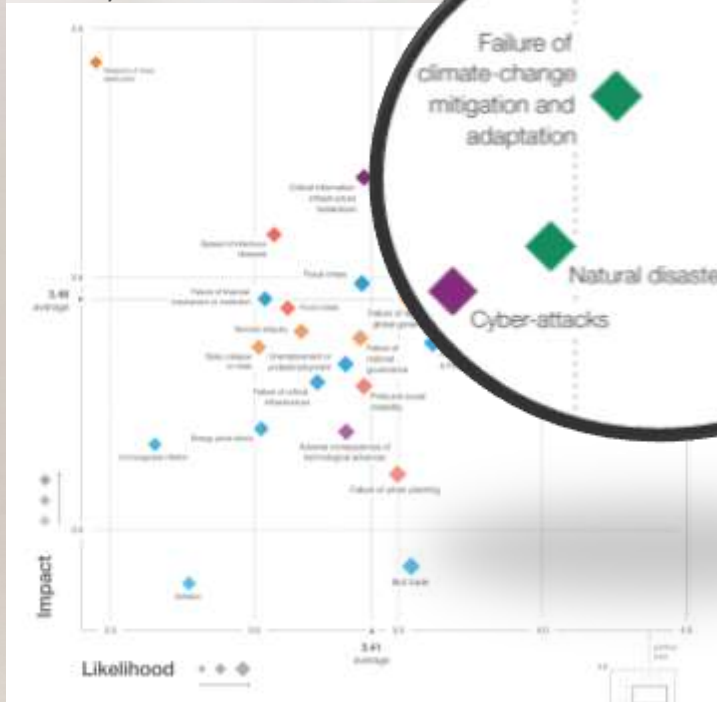# ....Cyber Security – Global Challenge

World Economic Forum –
Global Risk Report
January 2019

Cyber Attacks –
#4 Global Risks
#1 Man Made Risk

46% of all companies were affected
36% of all consumers globally lost data

[Internal Use] for Check Point employees

WHY?

#1 Detection mentality

DETECTION!

If you accept detection
you've already lost

Generations of Attacks and Protections

Gen I
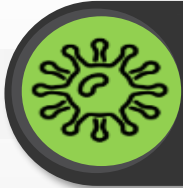
Virus

Late 1980s –
PC attacks - standalone

The Anti Virus

Gen II

Networks

Mid 1990s –
Attacks from the internet

The Firewall

Gen III

Applications

Early 2000s -
Exploiting vulnerabilities
in applications

Intrusion
Prevention (IPS)

Gen IV

Payload

2010 -
Polymorphic Content

Behavioral
Analysis

WELCOME TO THE FUTURE OF CYBER SECURITY

GEN V ATTACKS

Large scale (across country and industry)

Multi-vector (network, cloud, mobile)

Commercial & Government Grade Attack tools

GEN V VULNERABILITIES

16,555 vulnerabilities found in 2018 (up from 6,447 in 2016)

736 Mobile (iOS & Android) vulnerabilities in 2018
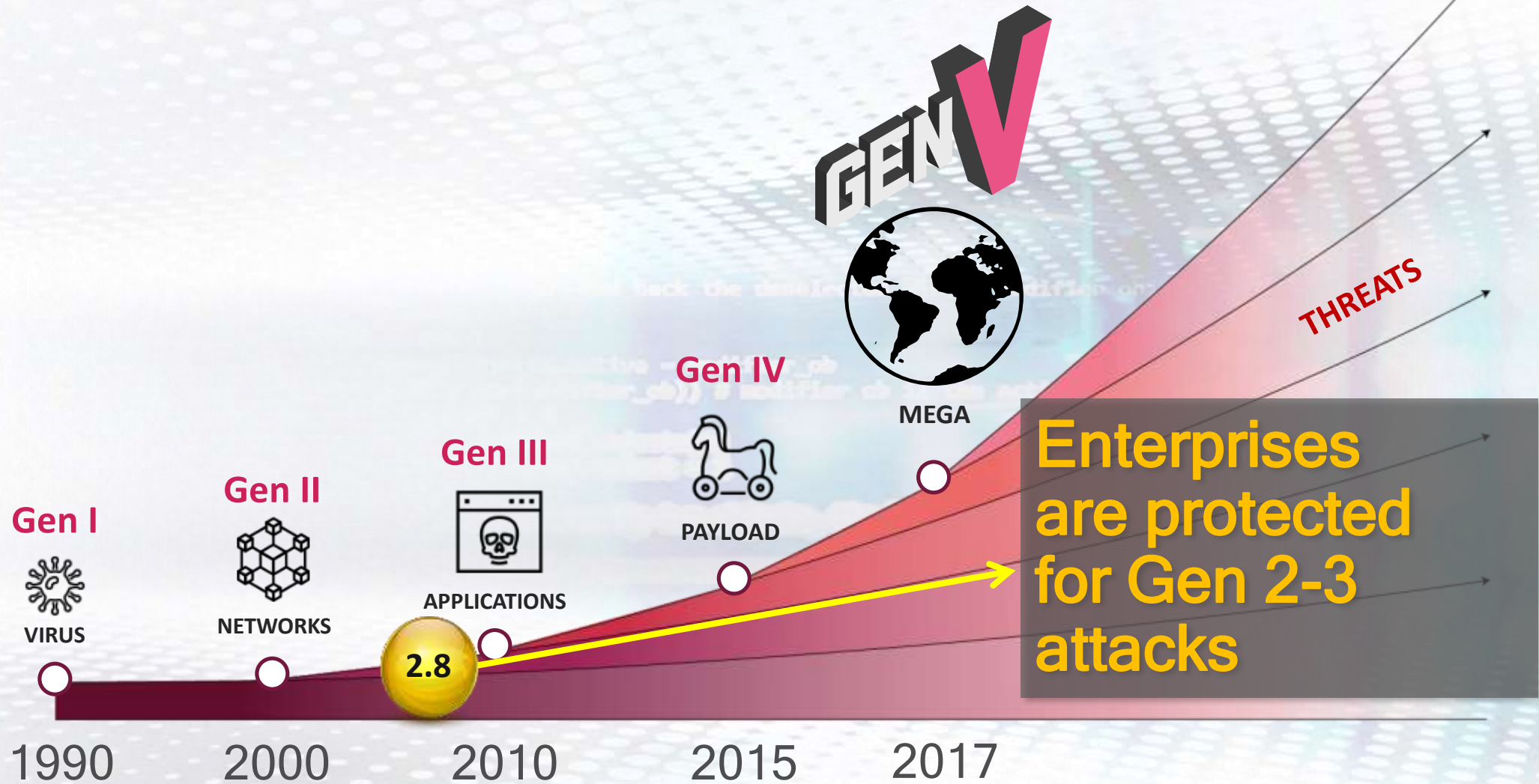
Cloud Infrastructure is the weakest link

Check Point
SOFTWARE TECHNOLOGIES LTD

#2 – Not protected to current level attacks

GEN V

MEGA

Gen IV

PAYLOAD

Gen III

APPLICATIONS

Gen II

NETWORKS

Gen I

VIRUS

2.8

THREATS

Enterprises are protected for Gen 2-3 attacks

1990   2000   2010   2015   2017

[Internal Use] for Check Point employees

#3 Too much complexity

Too many different solutions

	2007	2018
Threat Actors	<50	>1,000
Threat Types	<50	>1,000,000
Alerts / Day (Average Per Firm)	<1,000	>1,000,000
Security Vendors	<100	>2,600

Source: Former CIA director Gen (Ret) David H. Petraeus, CyberTech, Jan 2018

Solutions do not cooperate –
no shared intelligence or architecture

Complexity - Preventing Infected Files

Complexity – Broader View

16 ATTACK VECTORS

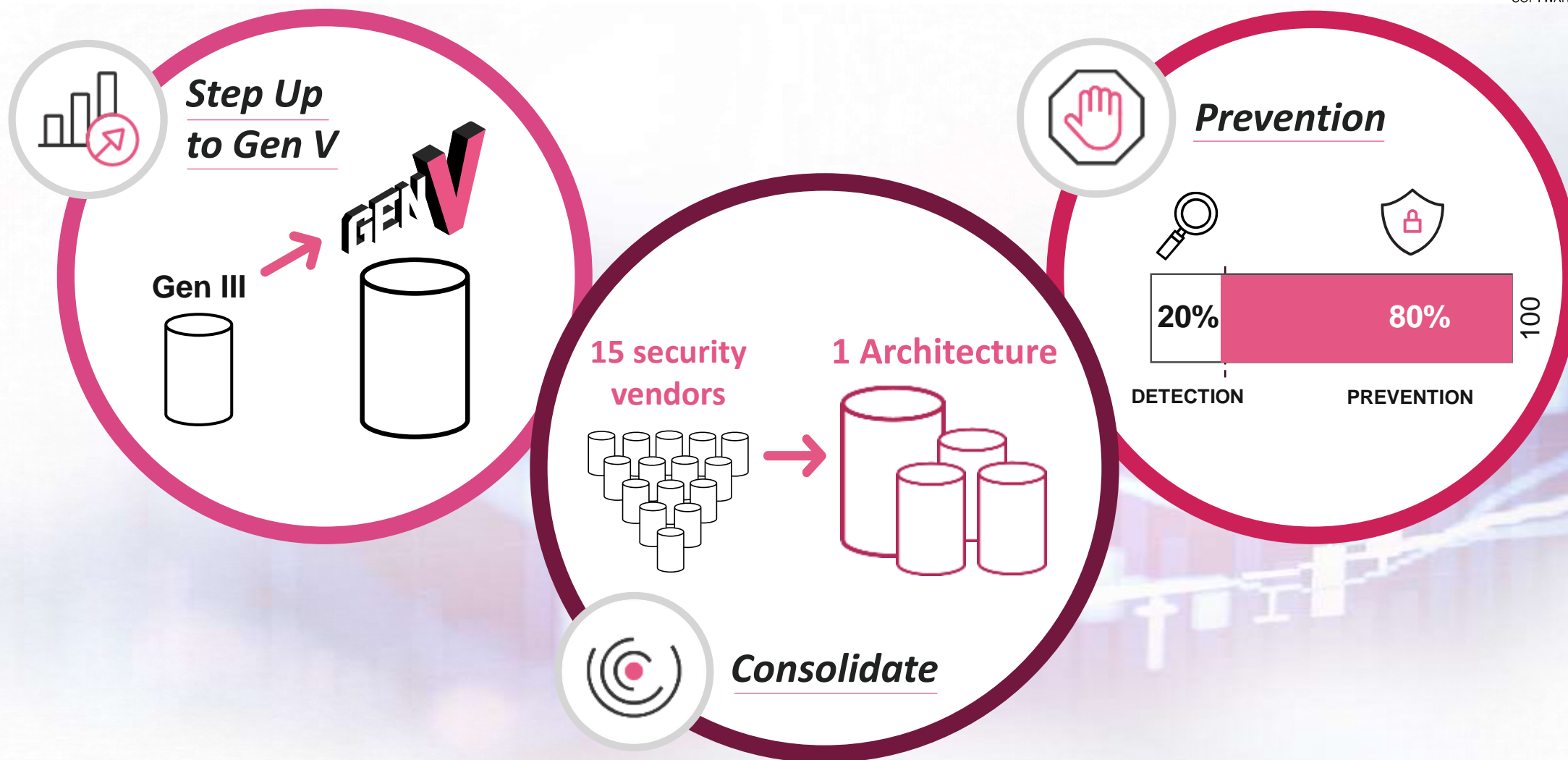**26 SECURITY TECHNOLOGIES**

Security Technology	Business Email	Perimeter	End Point	Mobile	Web Browsing	Data Center	Cloud IaaS	Cloud SaaS	Messaging Apps	Branch Office	Web Server	IoT	USB Storage	Database	FTP/File Share	Private Email	Vector 1	Vector 2	Vector 3
Firewall		☠	☠			☠	☠	☠		☠		☠							
Identity Access Management		☠					☠	☠								☠			
Remote Access			☠	☠		☠	☠					☠							
DDOS					☠	☠	☠				☠	☠		☠	☠	☠			
Site to Site IPSec		☠				☠	☠												
URLF		☠	☠	☠															
App Control		☠	☠									☠							
IPS		☠	☠	☠	☠	☠	☠			☠	☠			☠		☠			
WAP					☠	☠		☠			☠			☠		☠			
Anti Virus	☠	☠	☠	☠	☠	☠							☠	☠		☠			
Anti Bot			☠	☠	☠	☠													
File Emulation & Anti-Exploit	☠	☠	☠	☠		☠	☠							☠	☠	☠			
File Extraction	☠	☠	☠	☠	☠	☠								☠	☠	☠			
Anti Ransomware	☠	☠	☠											☠					
DLP	☠	☠						☠						☠	☠	☠			
Doc Security	☠		☠												☠				
Phishing	☠	☠		☠												☠			
Account Take Over		☠	☠																
Man in the Middle			☠	☠															
Password Leak			☠											☠					
Micro Segmentation					☠		☠												
SSL & TLS Inspection		☠			☠	☠										☠			
Compliance		☠	☠	☠										☠					
Application Scan				☠															
Disk & Media Encryption				☠									☠	☠					
Forensics		☠		☠		☠	☠			☠				☠					
Future 1																			
Future 2																			
Future 3																			

HOW CAN
WE ADDRESS
THIS TREND?

Step Up to Gen V

Gen III → Gen V

Consolidate

15 security vendors → 1 Architecture

Prevention

20% DETECTION | 80% PREVENTION | 100

Step Up Your Security Level from Gen III to Gen V

Gen III

GEN V

[Internal Use] for Check Point employees

Simplify and Consolidate your Security

15
SECURITY VENDORS

CONSOLIDATE

1 Architecture
5-6 Vendors

[Internal Use] for Check Point employees
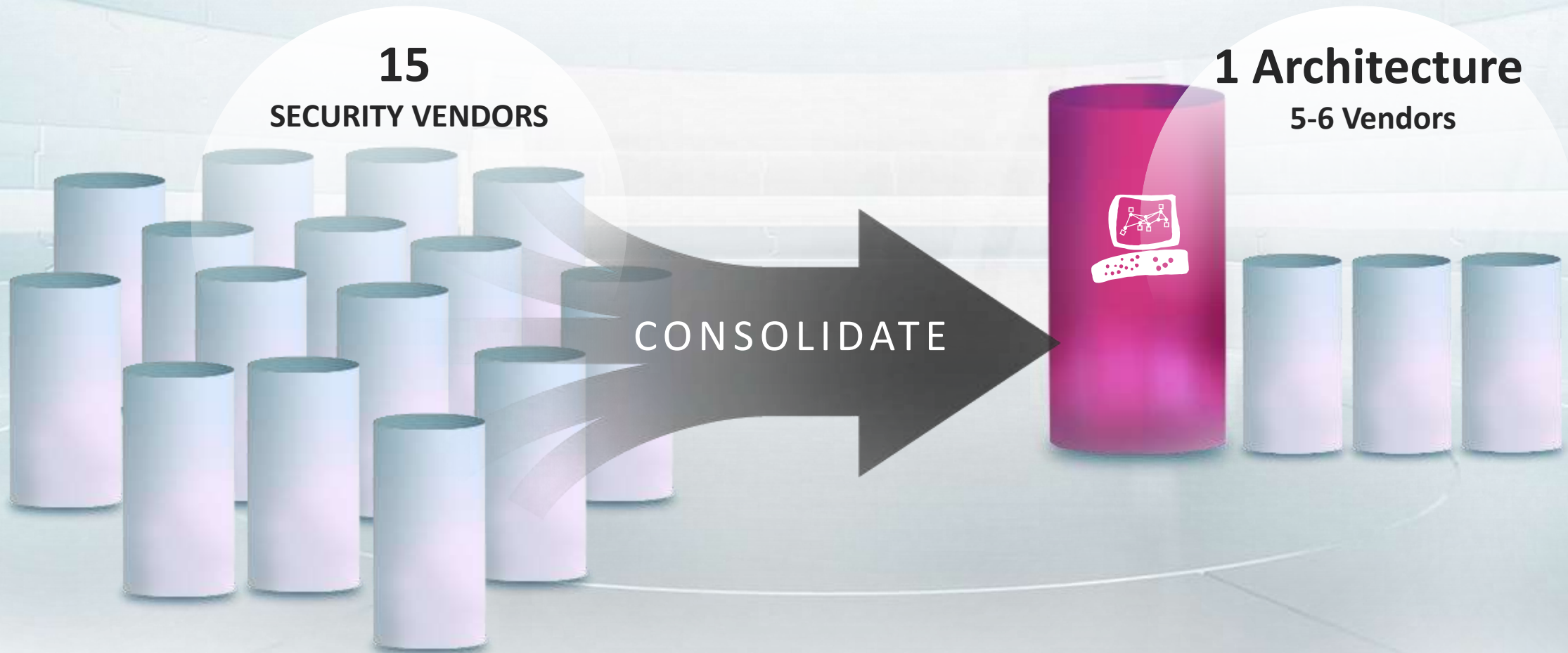
New Investment in Cyber Security

20% 0% 80% 20%

DETECTION

PREVENTION

0

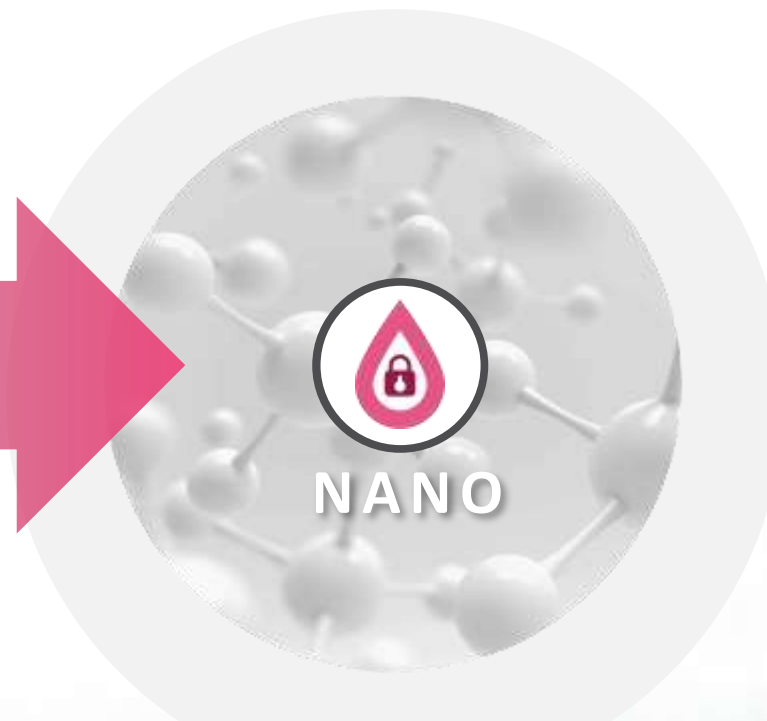100

[Restricted] for designated teams
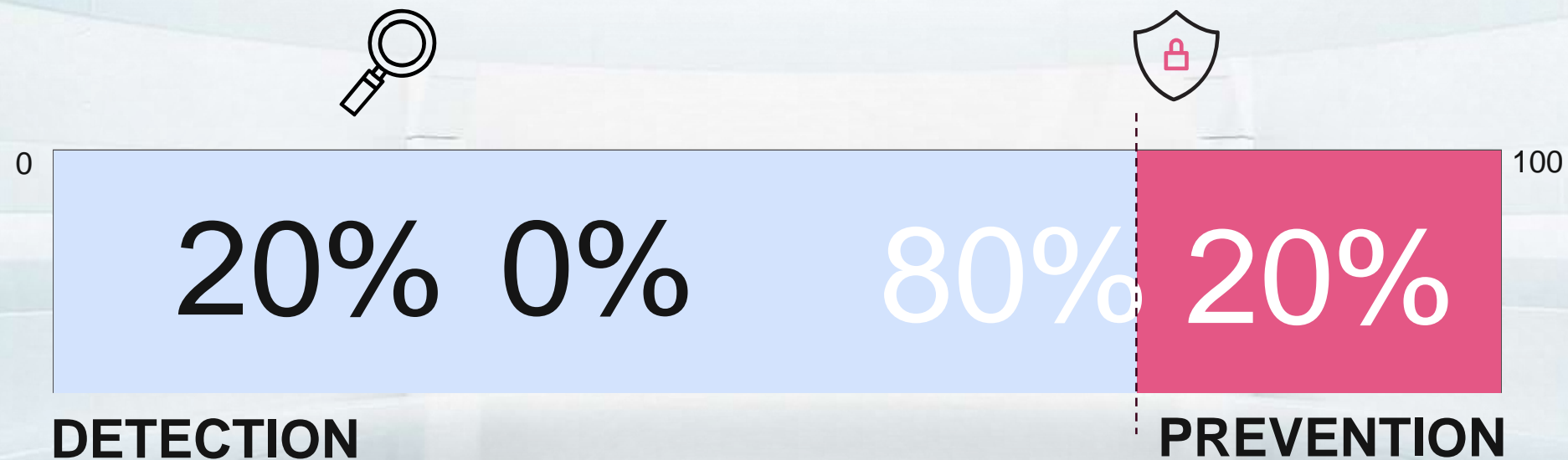
WHAT'S
NEXT?

Tightly coupled
monolithic Security

Security Service
and Delivery

BIG: Multi-core,
multi-gigabyte

NANO

Decouple Security Delivery and Service
Nano-Agent – Everywhere – Cloud, IoT
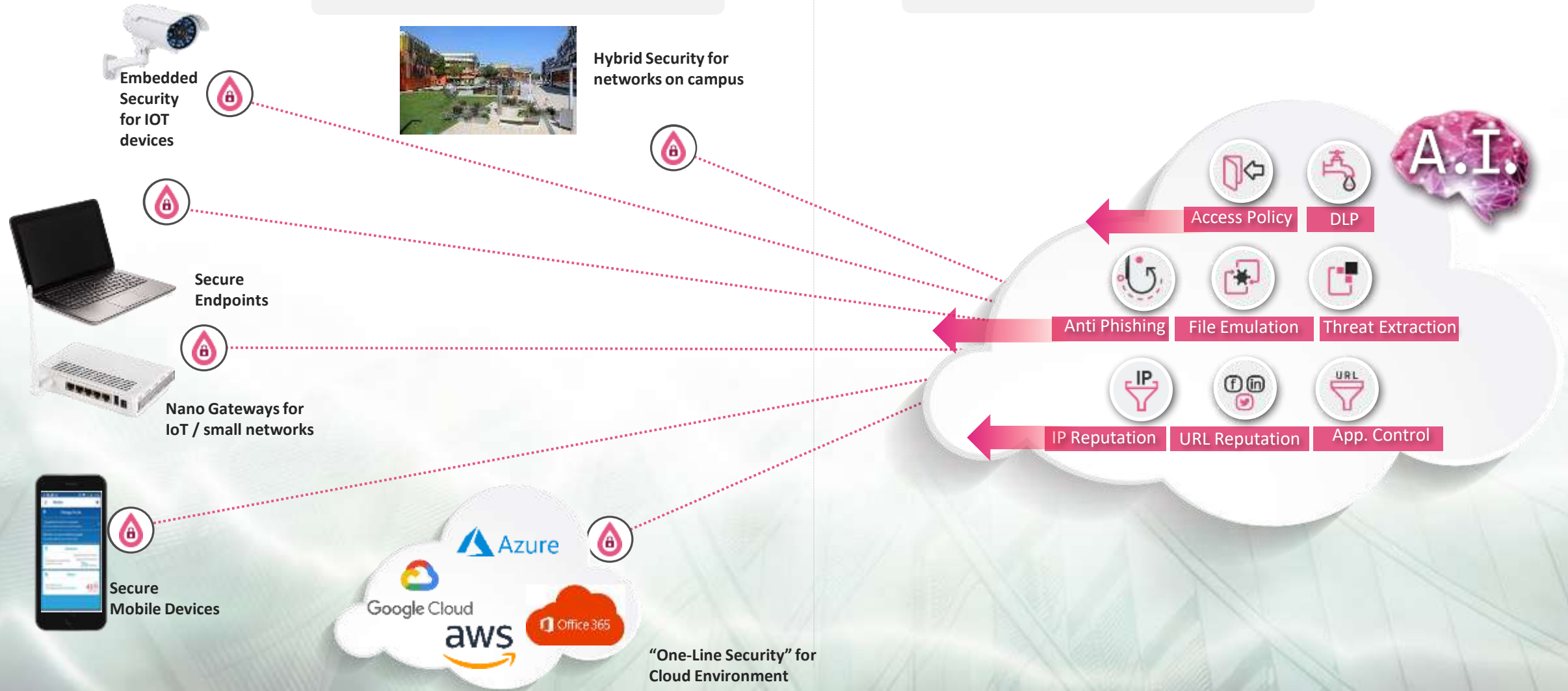
Future: Cloud Security Architecture

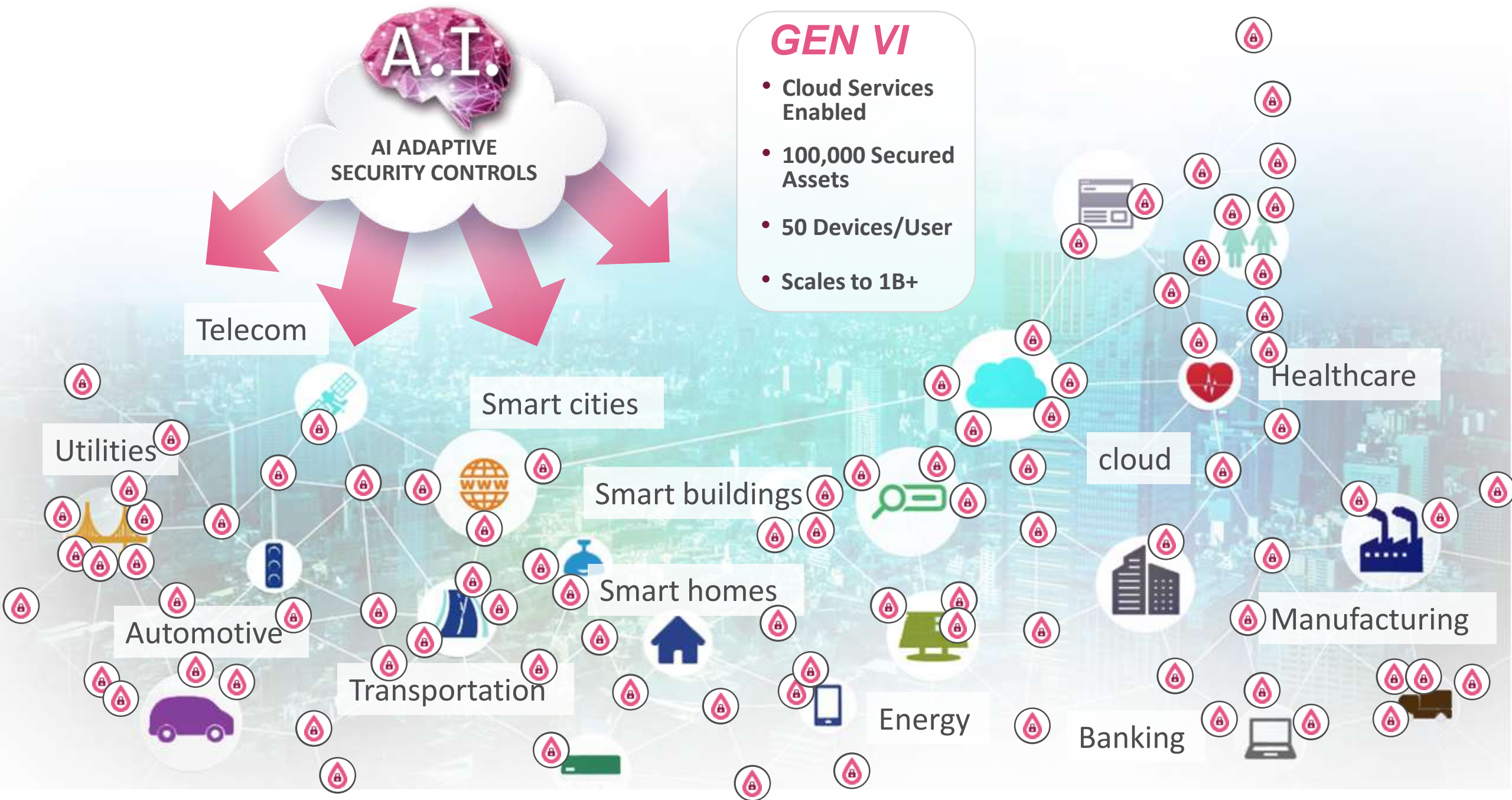**Hybrid/Cloud Delivered Security Services and Security Delivery**
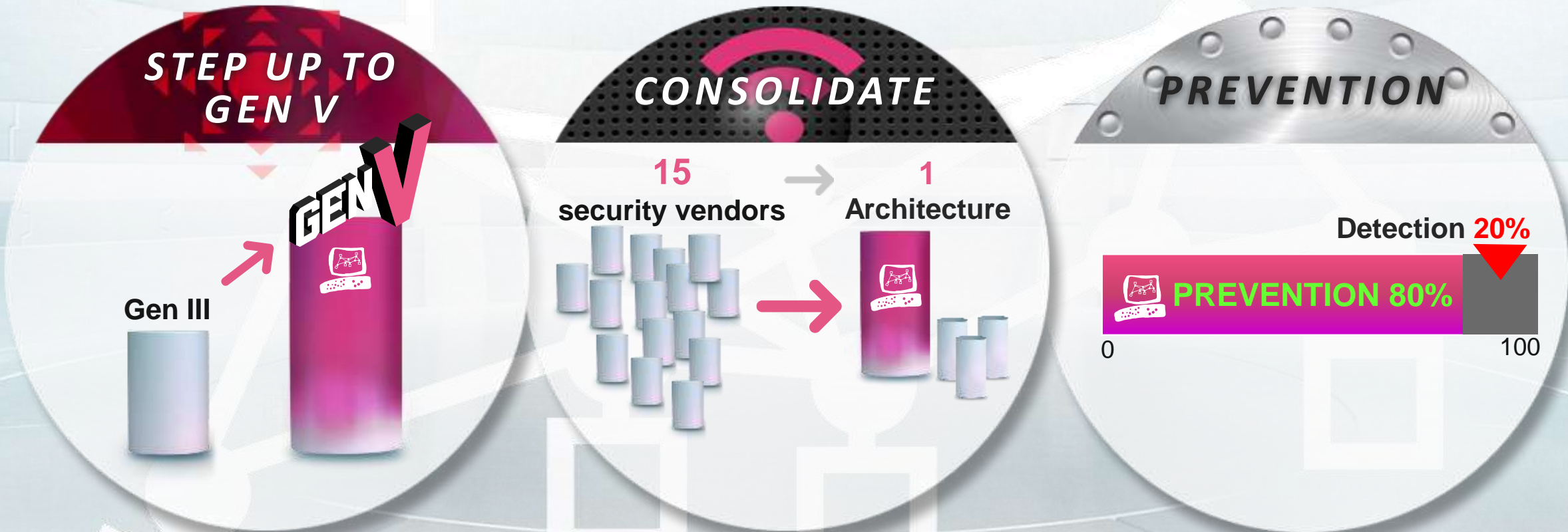
SECURITY DELIVERY

SECURITY SERVICES

Embedded Security for IOT devices

Hybrid Security for networks on campus

Secure Endpoints

Nano Gateways for IoT / small networks

Secure Mobile Devices

A.I.

Access Policy

DLP

Anti Phishing

File Emulation

Threat Extraction

IP Reputation

URL Reputation

App. Control

Azure

Google Cloud

aws

Office 365

"One-Line Security" for Cloud Environment

WELCOME TO THE FUTURE OF CYBER SECURITY

AI ADAPTIVE
SECURITY CONTROLS

GEN VI

- **Cloud Services Enabled**
- **100,000 Secured Assets**
- **50 Devices/User**
- **Scales to 1B+**

Telecom

Smart cities

Healthcare

Utilities

cloud

Smart buildings

Smart homes

Manufacturing

Automotive

Transportation

Energy

Banking

TO SUMMARIZE...

Summary

Check Point®
SOFTWARE TECHNOLOGIES LTD

STEP UP TO GEN V

GEN V

Gen III

CONSOLIDATE

15 → **1**
security vendors → Architecture

PREVENTION

Detection **20%**

PREVENTION 80%

0   100

[Restricted] for designated teams

WELCOME TO THE FUTURE OF CYBER SECURITY